

Parallelized Attacks on Elliptic Curve Discrete Logarithm Problem

Qin ZHOU, Liang XIA
fatestudio@gmail.com, liangxia2006@gmail.com

University of California, Santa Barbara

March 5, 2013

Elliptic Curve (on Finite Field p)

- Elliptic Curve $E : y^2 = x^3 + Ax + B \pmod{p}$

- Nodes: $P = (x, y) \in E, x, y \in \mathbb{Z}_p^*$

- Define addition operation on EC nodes:

$$P_1 + P_2 = (x_1, y_1) + (x_2, y_2) = P_3 = (x_3, y_3)$$

$$x_3 = m^2 - x_1 - x_2$$

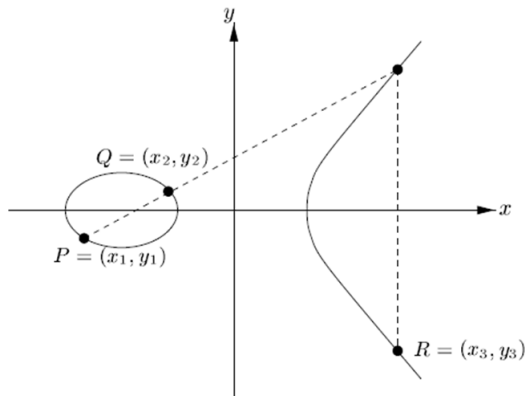
$$y_3 = m(x_1 - x_3) - y_1$$

$$m = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & P_1 \neq P_2 \\ (3x_1^2 + b)/(2y_1) & P_1 = P_2 \end{cases}$$

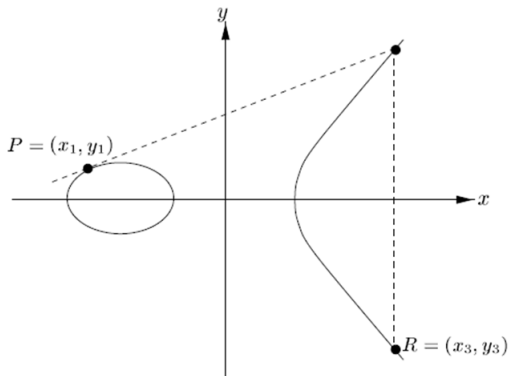
If the slope m is infinite, then $P_3 = \infty$. There is one additional law: $\infty + P = P$ for all points P

- Nodes set \mathbb{P} with addition operation $+$ forms a **Abelian Group**

Addition: $P_1 + P_2 = P_3$ ($P + Q = R$)



Addition: $P + P = 2P$



Elliptic Curve Discrete Logarithm Problem (ECDLP)

- If we have a curve E , a node P , and a number k , calculate kP is easy: $(k, P) \rightarrow kP$

e.g. Using **binary method of exponentiation** to compute $254P$:

$$P \xrightarrow{d} 2P \xrightarrow{a} 3P \xrightarrow{d} 6P \xrightarrow{a} 7P \xrightarrow{d} 14P \xrightarrow{a} 15P \xrightarrow{d} 30P \xrightarrow{a} 31P \xrightarrow{d} 62P \xrightarrow{a} 63P \xrightarrow{d} 126P \xrightarrow{a} 127P \xrightarrow{d} 254P$$

- However, If we have kP and P , get k is **hard**: $(kP, P) \not\rightarrow k$

Applications of ECDLP

- Example: Elliptic Curve Diffie Hellman (ECDH)

Share a secret $k_a k_b P$ between Alice and Bob preventing Eve

Alice

private key: k_a

public key: $k_a P$

$k_a P \xrightarrow{\text{to Bob}}$

Shared key: $k_a * k_b P = k_a k_b P$

Bob

private key: k_b

public key: $k_b P$

$\xleftarrow{\text{to Alice}} k_b P$

Shared key: $k_b * k_a P = k_a k_b P$

- Other Examples: EC Digital Signature Authentication (ECDSA), EC ElGamal

Why use Elliptic Curve?

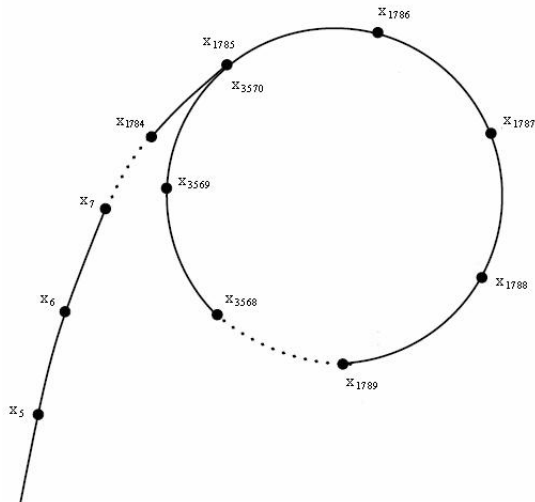
- Using much less bits while achieving the same Level security compared to RSA (160 bits of ECC \approx 1024 bits of RSA)
- Less bits means less bandwidth usage and better performance

Attacking ECDLP

Attacking Methods

- 1. Exhaustive Key Search (Time: $O(n)$, n is the order of P ; Space: $O(1)$)
- 2. Baby Step, Giant Step (Time: $O(\sqrt{n})$; Space: $O(\sqrt{n})$)
- 3. Pollard's ρ Method (Time: $O(\sqrt{\pi n/2})$; Space: negligible)
- 4. Distributed version of Pollard's ρ algorithm (Time: $O(\sqrt{\pi n/2}/2m)$; Space: negligible)
- 5. Pohlig-Hellman Method (Need factoring, which is hard)
- ...

Pollard ρ Method



Parallel Pollard Rho (van Oorschot and Wiener)

- With m processors, m pseudo-random walks starting at $X_o^{(i)} = a_i P + b_i Q$
- Each processor need to compute $O(\sqrt{\pi n/2}/m)$ iterations
- Central server need to store all $O(\sqrt{\pi n/2})$ points
- Define distinguished points $S_D \subset G$ and $\theta = |S_D|/|G|$
- Processors only send distinguished points to central server
 $O(\frac{\sqrt{\pi n/2}}{m} + \frac{1}{\theta})$ time $O(\theta\sqrt{\pi n/2})$ space





Challenges

- Build everything from scratch (because standardized Elliptic Curves are too large to break)
- Efficiently find the order of G
- Build parallelized attacking framework




Steps of implementation

- Set the maximum number of bits N . All numbers in this implementation are smaller than 2^N
- generate A , B and a prime p to form a Elliptic Curve
- randomly find a base G
- get the order of this G ($nG = \infty$)
- choose a random k that $0 \leq k < n$ as the private key and compute kG as the public key
- implement attacks

Reference

-  "Certicom ECC Challenge", http://www.certicom.com/images/pdfs/cert_ecc_challenge.pdf
-  D. McGrew, K. Igoe and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC6090
-  Diffie, W. and M. Hellman, "New Directions in Cryptography", IEEE Transactions in Information Theory IT-22, pp. 644-654, 1976.
-  ElGamal, T., "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, Vol. 30, No. 4, pp. 469-472, 1985.

Reference

-  L. C. Washington, "Elliptic Curves Number Theory and Cryptography", Second Edition, 2008
-  Junfeng Fan, et, "Breaking Elliptic Curve Cryptosystems using Reconfigurable Hardware", 2010
-  DV Bailey, "Breaking ECC2K-130", 2010